Theoretical Computer Science 411 (2010) 1115–1120

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

On the problem of freeness of multiplicative matrix semigroups

Paweł Gawrychowski [a], Marin Gutan [b], Andrzej Kisielewicz [c,*]

[a] University of Wrocław, Institute of Computer Science, ul. Joliot-Curie 15, 50-383 Wrocław, Poland
[b] Université Blaise Pascal, Laboratoire de Mathématiques, 63177 Aubière Cedex, France
[c] University of Wrocław, Institute of Mathematics, pl. Grunwaldzki 2, 50-384 Wrocław, Poland

ARTICLE INFO

Article history:
Received 17 September 2008
Received in revised form 28 November 2009
Accepted 5 December 2009
Communicated by B. Durand

Keywords:
Matrix semigroups
Freenes
Decidability

ABSTRACT

The following problem looking as a high-school exercise hides an unexpected difficulty. Do the matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 3 & 5 \\ 0 & 5 \end{pmatrix}$$

satisfy any nontrivial equation with the multiplication symbol only? This problem was mentioned as open in Cassaigne et al. [J. Cassaigne, T. Harju, J. Karhumäki, On the undecidability of freeness of matrix semigroups, Internat. J. Algebra Comput. 9 (3–4) (1999) 295–305] and in a book by Blondel et al. [V. Blondel, J. Cassaigne, J. Karhumäki, Problem 10.3: Freeness of multiplicative matrix semigroups, in: V. Blondel, A. Megretski (Eds.), Unsolved Problems in Mathematical Systems and Control Theory, Princeton University Press, 2004, pp. 309–314] as an intriguing instance of a natural computational problem of deciding whether a given finitely generated semigroup of 2×2 matrices is free. In this paper we present a new partial algorithm for the latter which, in particular, easily finds that the following equation

$$AB^{10}A^2BA^2BA^{10} = B^2A^6B^2A^2BABABA^2B^2A^2BAB^2$$

holds for the matrices above.[1] Our algorithm turns out quite practical and allows us to settle also other related open questions posed in the mentioned article.

1. Introduction

The product of matrices is one of the most fundamental operations used in computational practice and theoretical computer science. Therefore there is a wide interest among computer scientists in various practical and theoretical problems concerning matrices, including more or less detailed algorithmic issues. In particular, a number of natural decision problems concerning semigroups generated by integer matrices have been studied. For example, one asks, given a finite set of $n \times n$ integer matrices, if the semigroup generated by these matrices is free, or contains the null matrix, or contains the identity matrix, or is a group, etc. Some of these problems where shown to be undecidable, for some subproblems' algorithms were found, while some cases are still open. We refer the reader to [2,1,4,6,5] for more details.

* Corresponding author. Tel.: +48 713222206.
E-mail addresses: gawry1@gmail.com (P. Gawrychowski), Marin.Gutan@math.univ-bpclermont.fr (M. Gutan), Andrzej.Kisielewicz@math.uni.wroc.pl (A. Kisielewicz).

[1] This equation has been obtained also by the mean of heavy computations by Cassaigne and Nicolas and reported earlier in the preprint [5] (see the remark in Section 1).

0304-3975/$ – see front matter
doi:10.1016/j.tcs.2009.12.005

In this paper, we consider the problem of deciding whether a given finitely generated semigroup of 2×2 matrices (with rational entries) is free, or equivalently, whether a given morphism of the free semigroup $\{a_0, a_1, \ldots, a_{k-1}\}^+$ into the multiplicative semigroup of 2×2 matrices is an embedding. The corresponding problem for 3×3 matrices is undecidable: in [7] it was shown that it is undecidable whether the semigroup generated by a finite number of 3×3 nonnegative integer matrices is free; in [3] the result was improved by showing that the problem remains undecidable even if we require that the matrices are upper-triangular. In the latter paper the problem is considered also for 2×2 matrices. This case is especially intriguing. On the one hand, it was shown in [3] that the method applied in case $n = 3$ cannot work for $n = 2$. On the other hand, it is known that all finitely generated free semigroups can be embedded into a 2-generator matrix semigroup (over nonnegative integers), and freeness is a well-known decidable property for finitely generated subsemigroups of free semigroups. One of such embeddings is given by mapping each generator a_i onto matrix $\begin{pmatrix} k & i \\ 0 & 1 \end{pmatrix}$, where $i = 0, 1, \ldots, k-1$. It is easy to check that this is an embedding indeed. But in the very simple case of two generators a and b mapped onto the matrices A and B given in the abstract the question has been open.

In order to introduce the reader to the essence of this problem we summarize the result of [3] concerning the case 2×2 matrices. In fact the authors looking for a decidable subproblem study only a restricted case of the problem of two upper-triangular matrices A and B with rational entries, that is, the matrices of the form:

$$A = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}.$$

They observe first that in this case one can assume that both the matrices are invertible; otherwise, as it is easy to see, they satisfy either equation $A^2BA = ABA^2$ or equation $B^2AB = BAB^2$, and therefore the semigroup $\{A, B\}^+$ generated by A and B is not free. Furthermore, if one of the matrices is a power of the second then the generated semigroup can be free, but with one free generator. Thus, in what follows referring to "free semigroup" we mean "free with two free generators".

Now, an important reduction is given by [3, Proposition 1], which shows that we may in fact restrict to the matrices of the form

$$A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b & 1 \\ 0 & 1 \end{pmatrix},$$

where a, b are rational numbers other than $-1, 0, 1$. Thus, the instance of so restricted problem may be encoded by a pair of rational numbers (a, b). By [3, Lemma 4] the instances (a, b), (b, a), $(\frac{1}{a}, \frac{1}{b})$, $(\frac{1}{b}, \frac{1}{a})$ are equivalent: they have the same answer, and if one of the pairs of corresponding matrices satisfies a nontrivial equation, then equation for other pairs may be obtained (easily) from the former. Another useful observation is that if matrices A, B satisfy any nontrivial equation $U = V$, then one may assume that the left-hand side U starts from A and the right-hand side V starts from B, and consequently, A, B satisfy the nontrivial equation $UV = VU$ in which the number of occurrences of A and B on both the sides is the same (i.e., UV and VU are commutatively equivalent). It follows, that $\{A, B\}^+$ is free if and only if $\{\lambda A, \mu B\}^+$ is free (for any nonzero rational λ and μ). In particular, each instance of the problem with rational entries is equivalent to one with integer entries.

Let A and B be as above, and let $v_p(x)$ denotes the *p-adic valuation* of x (defined by $v_p(p^n y/z) = n$ for a prime p and integers n, y, z such that y and z are not divisible by p). Then, each of the following two conditions

(i) *there is a prime p such that* $v_p(a) > 0$ *and* $v_p(b) > 0$;
(ii) $|a| + |b| \leq 1$

is sufficient for the semigroup $\{A, B\}^+$ to be free. These results established in Propositions 1 and 2 of [3] are a base for a partial algorithm to check whether a semigroup generated by A and B is free. The algorithm always terminates with a correct answer when the semigroup is not free, but in the opposite case it may never terminate. In particular, the algorithm described in [3] is not effective enough to settle the case of the matrices $\begin{pmatrix} \frac{2}{3} & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} \frac{3}{5} & 1 \\ 0 & 1 \end{pmatrix}$, or equivalently matrices $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ and $\begin{pmatrix} 3 & 5 \\ 0 & 5 \end{pmatrix}$. The authors claim only that the algorithm does not terminate in a reasonable time for the instance $(\frac{2}{3}, \frac{3}{5})$, and that the corresponding matrices do not satisfy any equation where the lengths of both the sides are at most 20.

In the conclusion of [1] the authors hope that they pointed out a problem which is not only very simply formulated, but also fundamental and challenging. Agreeing with this opinion we undertook our study, concentrating on intriguing simple questions left open in [3].

In the next section we reduce the problem considered in [3] to finding a solution of an exponential diophantine equation. In Section 3 we describe the algorithm that works faster than the one described in [3] and report some computational results. In Section 4, using techniques developed for the algorithm, further sufficient conditions for freeness are formulated.

Remark. As mentioned in the abstract, our algorithm finds, in particular, an equation satisfied by the matrices above. The same equation (which is the shortest possible nontrivial equation for these matrices) has been found independently, and in a different way, by Cassaigne and Nicolas. As reported in the preprint [5], they have obtained it by "the mean of heavy computations". We thank one of the referees for bringing our attention to this fact. In general, [5] can be recommended to the reader as a good survey on the decidability of freeness problems over various particular semigroups, containing both new results and a number of challenging open problems in the area.

2. Exponential diophantine equations

If invertible matrices A and B satisfy any nontrivial equation in the multiplicative semigroup they generate, then obviously they satisfy also an equation of the form

$$A^{k_1}B^{m_1}A^{k_2}B^{m_2}\dots A^{k_u}B^{m_u}A^{k_{u+1}} = B^{s_1}A^{r_1}B^{s_2}A^{r_2}\dots B^{s_w}A^{r_w}, \tag{1}$$

where $k_i, m_i, s_j, r_j > 0$ for all $1 \le i \le u$ and $1 \le j \le w-1$, $s_w > 0$, and $k_{u+1}, r_w \ge 0$. Let

$$A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b & 1 \\ 0 & 1 \end{pmatrix} \tag{2}$$

with rational $a, b \ne -1, 0, 1$. Then, computing both the sides of (1) and comparing the right-upper corners of the obtained matrices we obtain (after multiplying by $1-b$) the following equation

$$\begin{aligned} &a^{k_1}(1-b^{m_1}) + a^{k_1+k_2}b^{m_1}(1-b^{m_2}) + \cdots + a^{k_1+\cdots+k_u}b^{m_1+\cdots+m_{u-1}}(1-b^{m_u}) \\ &\quad = (1-b^{s_1}) + a^{r_1}b^{s_1}(1-b^{s_2}) + \cdots + a^{r_1+\cdots+r_{w-1}}b^{s_1+\cdots+s_{w-1}}(1-b^{s_w}) \end{aligned} \tag{3}$$

We note that neither k_{u+1} nor r_w occurs in this equation, so all the exponents occurring in the equation are positive. Another form of this equation reads

$$a^{k_1}(1-b^{m_1}(1-a^{k_2}(1-b^{m_2}(\dots)))) + b^{s_1}(1-a^{r_1}(1-b^{s_2}(1-a^{r_2}(\dots)))) = 1, \tag{4}$$

where the first term on the left-hand side ends with b^{m_u}, and the right-hand side ends with b^{s_w}. Let us note that conditions (i) and (ii) in the previous section are straightforward consequences of (3) and (4).

If we assume that both the sides in Eq. (1) are commutatively equivalent, that is

$$\sum k_i = \sum r_i \quad \text{and} \quad \sum m_i = \sum s_i,$$

then the entries in the left-upper corners of the resulting matrices on both the sides are obviously equal. Therefore we have the following.

Theorem 2.1. *The multiplicative semigroup generated by matrices A and B of the form (2) is not free if and only if there exist positive integers u, w such that the exponential equation (3) (or equivalently Eq. (4)) has a solution in positive integers.*

This is an indication that the problem may be computationally very hard. At the same time (3) may be used to obtain some conditions on the exponents in the equation and thus to design a relatively efficient new partial algorithm. As we shall see the algorithm turns out quite practical in answering interesting questions.

Let us denote

$$L = \sum_{i=1}^{u} a^{k_1+\cdots+k_i}b^{m_1+\cdots+m_{i-1}}(1-b^{m_i}) \tag{5}$$

and

$$R = b^{s_1} - \sum_{i=1}^{w-1} a^{r_1+\cdots+r_i}b^{s_1+\cdots+s_i}(1-b^{s_{i+1}}) \tag{6}$$

so that (4) can be rewritten as

$$L + R = 1. \tag{7}$$

Generally L and R may be arbitrarily large and arbitrarily small, but under assumption $|a|, |b| < 1$ we may find the supremum and infimum of L and R, and using these to obtain conditions restricting the exponents. We need however to distinguish four cases with regard to whether a and b are positive or negative.

Lemma 2.2. *Let L and R be defined by (5) and (6), respectively, and assume that $|a|, |b| < 1$. Then for $u \ge 1$ and $v \ge 2$ the following hold:*

(i) *if both $a, b > 0$, then $L \in (0, a)$ and $R \in (0, b)$;*
(ii) *if $a < 0$ and $b > 0$, then $L \in (a, a^2)$ and $R \in (0, b(1-a))$;*
(iii) *if $a > 0$ and $b < 0$, then $L \in (0, a(1-b))$ and $R \in (b, b^2)$;*
(iv) *if both $a, b < 0$, then $L \in \left(\frac{a(1-b)}{(1-ab)}, \frac{a^2(1-b)}{(1-ab)}\right)$ and $R \in \left(\frac{b(1-a)}{(1-ab)}, \frac{b^2(1-a)}{(1-ab)}\right)$.*

Proof. One may show that in every case corresponding open intervals are given by the infimum and the supremum of L or R, respectively, considered for any fixed $u \geq 1$ and $w \geq 1$. Case (i) is easily seen from Eq. (4). For other cases one applies induction on u or w, respectively.

For example, for case (ii), we compute

$$L = a^{k_1}(1 - b^{m_1}) + a^{k_1} b^{m_1} \sum_{i=2}^{u} a^{k_2+\cdots+k_i} b^{m_2+\cdots+m_{i-1}}(1 - b^{m_i}),$$

which by induction hypothesis gives

$$\inf L = \inf\{a^{k_1}(1 - b^{m_1}) + a^{k_1} b^{m_1} a\} = \inf\{a^{k_1}(1 - b^{m_1}(1 - a))\} = a.$$

The other cases are similar. □

Lemma 2.2 corresponds closely to Lemma 2.2 of [3]. However, in contrast with the latter, our version shows that the cases (ii) and (iii) are symmetrical. This difference requires an explanation. The lack of symmetry in [3, Lemma 2.2] is caused by the fact that it includes, in a sense, cases corresponding to $u = 0$ and $v = 0, 1$ in which L and R may achieve exceptional extreme values. For the algorithm we make use of the fact that each matrix equation can be extended to a longer one so that looking for conditions on exponents we may ignore complications for initial values of u and v.

Another advantage is showing that the way expressions L and R are terminated does not influence the infima and maxima. In fact, L and R are almost symmetrical; they differ only in the number of terms in the sum, which for L is even, while for R is odd. A uniform version of the lemma (applied in our algorithm) is

Lemma 2.3. *If L is a finite sum of the form*

$$L = a^{k_1} - a^{k_1} b^{m_1} + a^{k_1+k_2} b^{m_1} - a^{k_1+k_2} b^{m_1+m_2} + \ldots,$$

where $|a|, |b| < 1$, then L satisfies the conditions (i–iv) *given in Lemma 2.2.*

3. Algorithm

Rather than giving a listing of a program or a pseudocode for it we describe the algorithm and the heuristics we use in it by an example for the case (1) with special comments for the unsolved case of $a = 2/3$ and $b = 3/5$.

First, applying suprema in Lemma 2.2(i) to Eq. (7) we obtain a restriction on values a and b

$$a + b > 1,$$

which is an instance of [3, Proposition 3]. Applying infima yields $0 < 1$, which produces no restriction in this case. Now, in order to obtain a condition on exponents k_1 and s_1 we rewrite Eq. (7) in the form

$$-a^{k_1}[b^{m_1}(1 - a^{k_2}) + a^{k_2} b^{m_1+m_2}(1 - a^{k_3}) + \cdots] - b^{s_1}[a^{r_1}(1 - b^{s_2}) + a^{r_1+r_2} b^{s_2}(1 - b^{s_3}) + \ldots] = 1 - a^{k_1} - b^{s_1}. \quad (8)$$

Applying Lemma 2.3(i) for the expressions in square brackets we get

$$0 > 1 - a^{k_1} - b^{s_1}$$
$$-a^{k_1} b - b^{s_1} a < 1 - a^{k_1} - b^{s_1}$$

which can be rewritten as

$$a^{k_1} + b^{s_1} > 1 > a^{k_1}(1 - b) + b^{s_1}(1 - a). \quad (9)$$

There are only finitely many pairs k_1 and s_1 satisfying these inequalities. For example, in the case of $a = 2/3$ and $b = 3/5$ we get that $k_1, s_1 \leq 2$, and at least one of k_1, s_1 equals 1.

In order to find restrictions coming from valuations we use a modification of (8) with only one of a^{k_1} or b^{s_1} moved to the right-hand side.

$$a^{k_1}(1 - b^{m_1}) + a^{k_1+k_2} b^{m_1}(1 - b^{m_2}) + \cdots - a^{r_1} b^{s_1}(1 - b^{s_2}) - a^{r_1+r_2} b^{s_1+s_2}(1 - b^{s_3}) - \cdots = 1 - b^{s_1}. \quad (10)$$

For this form it is easily seen that if there is a prime p such that $v_p(a) > 0$ and $v_p(b) = 0$, then the p-adic valuation of the left-hand side of (10) is greater than or equal to $\min\{k_1, r_1\}$. Hence, we obtain

$$v_p(1 - b^{s_1}) \geq \min\{k_1, r_1\},$$

which restricts the set of possible values for s_1, k_1, and r_1. In fact, both the sides are divisible by $1 - b$, and we get a stronger condition after dividing (10) by this factor. We obtain

$$\begin{aligned} &a^{k_1}(1 + b + \cdots + b^{m_1-1}) + a^{k_1+k_2} b^{m_1}(1 + b + \cdots + b^{m_2-1}) + \cdots \\ &\quad - a^{r_1} b^{s_1}(1 + b + \cdots + b^{s_2-1}) - a^{r_1+r_2} b^{s_1+s_2}(1 + b + \cdots + b^{s_3-1}) - \cdots \\ &\quad = 1 + b + \cdots + b^{s_1-1}. \end{aligned} \quad (11)$$

In particular, $v_p(1+b+\cdots+b^{s_1-1})>0$, and consequently, $s_1>1$ (provided $v_p(a)>0$ and $v_p(b)=0$). For $a=2/3$, $b=3/5$ (and $p=2$), it means that $s_1=2$, and consequently, $k_1=1$. In a general case, the condition

$$v_p\left(\frac{1-b^{s_1}}{1-b}\right)\geq \min\{k_1,r_1\}$$

leads to conditions of the form $s_1\equiv k \pmod p$, which often considerably restricts the number of cases to be considered.

The next step in the algorithm is moving further terms on the right-hand side, assuming that now the equation is considered for fixed a^{k_1} or b^{s_1}. Namely, we write the equation in the form

$$\begin{aligned} &a^{k_1}b^{m_1}[a^{k_2}(1-b^{m_2})+a^{k_2+k_3}b^{m_2}(1-m^{m_3})+\cdots]+a^{r_1}b^{s_1}[b^{s_2}(1-a^{r_2})+a^{r_2}b^{s_2+s_3}(1-a^{r_3})+\cdots]\\ &\quad=1-a^{k_1}-b^{s_1}+a^{k_1}b^{m_1}+a^{r_1}b^{s_1}. \end{aligned} \tag{12}$$

For example, in the case of $a=2/3$ and $b=3/5$, with $k_1=1$ and $s_2=2$, we get now inequalities of the form

$$\frac{2}{3}b^{m_1}(1-a)+\frac{9}{25}a^{r_1}(1-b)<\frac{2}{75}<\frac{2}{3}b^{m_1}+\frac{9}{25}a^{r_1}.$$

From the first inequality it follows that $m_1,r_1\geq 5$, and from the other it follows, in particular, that $\min\{m_1,r_1\}\leq 7$. The progress in establishing exact values of exponents satisfying Eq. (1) is now slower, but with a help of computer one can find easily equation.

$$AB^{10}A^2BA^2BA^{10}=B^2A^6B^2A^2BABABA^2B^2A^2BAB^2$$

for the matrices (2) with $a=2/3$ and $b=3/5$. The fact that this equation holds one may check now even by hand.

Generally, in the algorithm we test larger and larger sequences of exponents given by inequalities and valuation conditions as above whether they satisfy Eq. (1). If there are no exponents satisfying the conditions, the algorithm terminates with answer "no equation". Comparing to the algorithm suggested in [3], it seems that introducing conditions on exponents rather than on sequences of matrices, and suitable generating of sequences of exponents, provides a logarithmic speed-up (also some techniques of dynamic programming are used). Anyway, while the algorithm in [3] is reported not to terminate in a reasonable time for the instance $a=2/3$ and $b=3/5$, our algorithm does. Finding the equation above and verifying that it is the shortest possible takes just a second on a modern computer (AMD Athlon XP 2600+ with 1GB of RAM).

We have checked also other unsettled cases suggested in [3, Figure 1]. The comments preceding [3, Figure 1] suggest that the unsettled cases are on the lines with slope $-9/10$ and $9/10$, and these are $(a,b)=(\pm 2/3,\pm 3/5)$ and $(a,b)=(\pm 1/2,\pm 5/9)$ (other cases on these lines are settled easily by earlier results). For $(a,b)=(-2/3,3/5)$, $(2/3,-3/5)$, $(-2/3,-3/5)$ the corresponding semigroup is never free, and the corresponding equations are

$$A^2B^6A^2BAB^2A^5=B^2AB^4A^2BA^4BA^3B$$
$$ABAB=B^2A^2$$
$$A^4BAB^2A^2B^2AB^2ABA^2B=B^2AB^3A^2BA^2BAB^2A^5.$$

(Apparently, the second of these cases was not considered carefully in [3]). For each of the cases $(a,b)=(\pm 1/2,\pm 5/9)$ the algorithm reports that the corresponding semigroup is free.

4. Further sufficient conditions for freeness

Using machinery worked out for the algorithm we can obtain some more general corollaries, and to answer another open question from [3].

Let $a=\frac{u}{v}$ and $b=\frac{x}{y}$ be an instance of the problem given by matrices (2), with $0<a,b<1$, and $\frac{u}{v},\frac{x}{y}$ irreducible fractions. We assume that $\gcd(u,x)=\gcd(v,y)=1$ and $a+b\geq 1$ (if this condition is not satisfied then by condition (i) (Section 1) the semigroup generated by A and B is free). We slightly generalize condition (ii) in this case.

Proposition 4.1. *Let $a=\frac{u}{v}$ and $b=\frac{x}{y}$ be as above, and assume in addition that there exists a prime p dividing u, but not dividing y. If $a+b^2\leq 1$, then the semigroup generated by matrices A and B given by (2) is free.*

Proof. Assume to the contrary that A,B satisfy Eq. (1). From (9) we have $a^{k_1}+b^{s_1}\geq 1$. Since $0<a,b<1$ and $a+b^2\leq 1$, we have $s_1=1$. It follows that the right-hand side of (11) is 1, and thus its p-valuation equals 0. Observing that the p-valuation of the left-hand side is greater than or equal to $k_1>0$ yields a desired contradiction. □

The instance $(\frac{3}{5},\frac{5}{8})$ involves three successive Fibonacci numbers $F(n)$. It seems interesting to consider a general pattern behind this instance, namely, all the instances of the form $(a,b)=(\frac{u}{v},\frac{v}{u+v})$ with $1<u<v$ and $\gcd(u,v)=1$. Applying the proposition above, $a+b^2\leq 1$ implies that in this case $a=\frac{u}{v}<\frac{-1+\sqrt{5}}{2}$. The right-hand side is the converse of the "golden ratio", and it is known that

$$\frac{F(2n)}{F(2n+1)}<\frac{-1+\sqrt{5}}{2}<\frac{F(2n+1)}{F(2n+2)}$$

for all $n > 0$. Consequently, the semigroups corresponding to instances $(a, b) = (\frac{3}{5}, \frac{5}{8}), (\frac{8}{13}, \frac{13}{21}), \ldots$ are all free. This is also true for instances $(\frac{5}{8}, \frac{8}{13}), (\frac{13}{21}, \frac{21}{34}), \ldots$, but to see this we need a deeper argument.

Proposition 4.2. *Let $a = \frac{u}{v}$ and $b = \frac{v}{u+v}$, where $2 < u < v$, and $\gcd(u, v) = 1$. If $a < 0.83$, then the semigroup generated by matrices A and B given by (2) is free.*

Proof. Assume to the contrary that A, B satisfy Eq. (1), and let p be the largest prime dividing u. From (9) we have $a^{k_1} + b^{s_1} \geq 1$.

We first show that $s_1 \geq 3$. Indeed, if $s_1 < 3$, then the right-hand side R' of (11) is either $R' = 1$ or $R' = 1 + b = \frac{u+2v}{u+v}$. In the case when $p > 2$, we have $v_p(R') = 0$, while for the left-hand side L', $v_p(L') > 0$, a contradiction. If $p = 2$, then by assumption, $u = 2^k$ with $k > 1$, and consequently, $v_p(R') \leq 1$, and $v_p(L') \geq 2$, which is again a contradiction proving the claim.

It follows that $a + b^3 \geq 1$. Observing that $b = \frac{1}{1+a}$, by an easy calculation, we obtain that $a^3 + 2a^2 - 2 \geq 0$, which yields $a > 0.83$. This contradiction completes the proof. $\square$

The experimental results of [3] on freeness of semigroups generated by two 2×2 upper-triangular matrices corresponding to instances (a, b) are summarized in [3, Figure 1]. The authors observe a striking symmetry in the picture. The symmetries with respect to the first diagonal or by inversion $(a, b) = (\frac{1}{a}, \frac{1}{b})$ follow from the established results. Yet, the authors have observed also the symmetries with respect to both axes: they claim that for all computed instances the answer for (a, b) is always the same as that for any $(\pm a, \pm b)$, and they have no explanation for this.

The proposition above yields a number of examples showing that, in fact, these symmetries fail. For example, let us note first that the equation $ABAB = BBAA$ for matrices (2), according to (3), is equivalent to $1 + b + ab = 0$. Hence, $b = -\frac{1}{1+a}$, and the semigroups corresponding to $(a, -\frac{1}{1+a})$ are never free. On the other hand, for $a = \frac{u}{v}$ we have $(\frac{u}{v}, \frac{v}{u+v}) = (a, \frac{1}{1+a})$, and by the proposition above, the corresponding semigroups for $a < 0.83$ (and $u > 2$) are free.

The smallest instance here is $(\frac{3}{5}, \frac{5}{8})$ and $(\frac{3}{5}, -\frac{5}{8})$. Applying our algorithm to $(-\frac{3}{5}, -\frac{5}{8})$ yields the equation

$$A^2B^{10}AB^2ABA^8 = B^2AB^5A^4B^3A^7B^3,$$

and applying it to $(-\frac{3}{5}, \frac{5}{8})$ reports that the semigroup is free. So the results are still symmetrical with respect to one of the axes. Yet, taking into account the symmetry with respect to the diagonal, that is, applying our considerations to pairs $(\pm\frac{5}{8}, \pm\frac{3}{5})$, shows that there is no symmetry with respect to any of the axes.

Acknowledgements

This research was done while the second author was visiting Université Blaise Pascal in Clermont-Ferrand. The results of the paper were presented in an invited talk at the AAA76 conference, Linz, May 23–25, 2008. This research was supported in part by Polish MNiSZW grant P03A 03430.

References

[1] V. Blondel, J. Cassaigne, J. Karhumäki, Problem 10.3: Freeness of multiplicative matrix semigroups, in: V. Blondel, A. Megretski (Eds.), Unsolved Problems in Mathematical Systems and Control Theory, Princeton University Press, 2004, pp. 309–314.
[2] O Bournez, M. Branicky, The mortality problem for matrices of low dimensions, Theory Comput. Syst. 35 (4) (2002) 433–448.
[3] J. Cassaigne, T. Harju, J. Karhumäki, On the undecidability of freeness of matrix semigroups, Internat. J. Algebra Comput. 9 (3–4) (1999) 295–305.
[4] J. Cassaigne, J. Karhumäki, Examples of undecidable problems for 2-generator matrix semigroups, Theoret. Comput. Sci. 204 (1–2) (1998) 29–34.
[5] J. Cassaigne, F. Nicolas, On the decidability of semigroup freeness, preprint, September 2008. available: arXiv:0808.3112v2 [cs.DM].
[6] Ch. Choffrut, J. Karhumäki, Some decision problems on integer matrices, Theor. Inform. Appl. 39 (1) (2005) 125–131.
[7] D. Klarner, J.-C. Birget, W. Satterfield, On the undecidability of the freeness of integer matrix semigroups, Internat. J. Algebra Comput. 1 (1991) 223–226.